In the Claims:

Please note the following current set of claims:

1. (Original) A method for providing cryptographic capabilities to a plurality of network users over a decentralized public network, the method comprising: (a) receiving a request for an access permission security profile on behalf of a network user; (b) authenticating the request; (c) creating the access permission security profile, to be used in forming a cryptographic key for enabling the network user to decrypt selected portions of an encrypted object and to encrypt selected portions of a plaintext object; and (d) securely transmitting the access permission security profile to the network user over the network.

2. (Original) The method of claim 1, wherein the creating step comprises: (i) identifying one or more groups of network users who are to be provided with cryptographic capabilities; (ii) establishing one or more access codes for each group, wherein each access code is adapted to be combined with other components to form a cryptographic key; and (iii) creating one or more security profiles for each network user, wherein each security profile contains at least one access code.

3. (Original) The method of claim 2, wherein each group is a category, organization, organization unit, role, work project, geographical location, workgroup or domain.

4. (Original) A method for providing decryption capabilities to a plurality of network users over a decentralized public network, the method comprising: (a) receiving a request for decryption capabilities on behalf of a network user; (b) authenticating the request; (c) creating an access permission security profile to be used in forming a cryptographic key for enabling the network user to decrypt an encrypted object; (d) receiving from the user information associated with the encrypted object; (e) generating a cryptographic key using the access permission security profile and the received information associated with the encrypted object; and (f) securely transmitting the cryptographic key to the network user over the network.

5. (Original) The method of claim 4, wherein the creating step includes: (i) identifying one or more groups of network users who are to be provided with cryptographic capabilities; (ii) establishing one or more access codes for each group, wherein each access code is adapted to be combined with other components to form a cryptographic key; and (iii) creating one or more security profiles for each network user, wherein each security profile contains at least one access code.

6. (Original) The method of claim 5, wherein each group is a category, organization, organization unit, role, work project, geographical location, workgroup or domain.

7. (Previously Amended) A method for cryptographically securing the distribution of information over a decentralized public network to a plurality of network users, the method comprising:

(a) creating a computer representable data object including one or more embedded

objects;

(b) selecting one or more embedded objects of the data object to be encrypted;

(c) encrypting the selected embedded objects;

(d) creating one or more access permission credentials;

(e) assigning an access permission credential to each of the selected embedded objects, wherein the access permission credential ensures that only authorized users are able to decrypt encrypted embedded objects of the data object;

(f) authorizing at least one network user from the plurality of network users; and

(g) transmitting the data object over the network.

8. (Original) The method of claim 7, wherein the information is digital content.

9. (Original) The method of claim 7, wherein the authorizing step includes: (i) receiving a request for an access permission security profile on behalf of a network user; (ii) authenticating the request; and (iii) securely transmitting the security profile to the network user over the network.

10. (Previously Amended) The method of claim 7, wherein the authorizing step includes: (i) sending a request for an access permission security profile on behalf of a network user to a centralized server system over the network; (ii) receiving the request at the central server system; (iii) authenticating the request; and (iv) securely transmitting the access permission security profile from the server system to the network user over the network.

11. (Previously Amended) The method of claim 7, wherein the authorizing step is automatic and based upon the user's possession of an access permission security profile.

12. (Original) The method of claim 7, wherein the encrypting step comprises: (i) identifying a group of network users who are to be allowed access to a data object to be encrypted; (ii) generating an appropriate cryptographic credential key from a set of credential categories, said credential key relating to the group of network users; (iii) generating a cryptographic working key from at least a domain component, a maintenance component, and a pseudorandom component; (iv) encrypting the data object with the working key; (v) encrypting the pseudorandom component with the credential key; and (vi) associating the encrypted pseudorandom component to the encrypted data object.

13. (Previously Amended) The method of claim 10 , wherein the access permission security profile is created by: (i) identifying one or more groups of network users who are to be provided with cryptographic capabilities; (ii) establishing one or more access codes for each group, wherein each access code is adapted to be combined with other components to form a cryptographic key; and (iii) creating one or more security profiles for each network user, wherein each security profile contains at least one access code.

14. (Original) The method of claim 13, wherein each group is a category, organization, organization unit, role, work project, geographical location, workgroup or domain.

15. (Original) The method of claim 1, 4 or 9, wherein the request is initiated in-band by the network user over the network.

16. (Original) The method of claim 1, 4, 9, 10, or 11, wherein the access permission security profile is in the form of a token that is adaptable to expire.

17. (Original) The method of claim 1, 4, 9, or 10, wherein the authenticating step includes the use of biometric identification.

18. (Original) The method of claim 1, 4, 9, or 10, wherein the authenticating step includes the use of a hardware token.

19. (Original) The method of claim 1, 4, 9, or 10, wherein the authenticating step includes the use of a software token.

20. (Original) The method of claim 1, 4, 9, or 10, wherein the authenticating step includes the use of a user password.

21. (Original) The method of claim 1, 4, 9, or 10, wherein the authenticating step includes the use of a record of time at which the request was made.

22. (Original) The method of claim 1, 4, 9, or 10, wherein the authenticating step includes the use of a record of the user's physical location.

23. (Cancelled)

24. (Cancelled)

25. (Cancelled)

26. (Cancelled)

27. (Cancelled)

28. (Cancelled)

29. (Cancelled)

30. (Cancelled)

31. (Cancelled)

32. (Cancelled)

33. (Cancelled)

34. (Cancelled)

35. (Cancelled)

36. (Cancelled)

37. (Cancelled)

38. (Cancelled)

39. (Cancelled)

40. (Cancelled)

41. (Cancelled)

42. (Cancelled)

43. (Cancelled)

44. (Cancelled)

45. (Cancelled)

46. (Cancelled).

47. (Cancelled).

48. (Cancelled)

49. (Cancelled)

50. (Cancelled)

51. (Cancelled)

52. (Currently amended) A centralized security management system for distributing cryptographic capabilities to a plurality of network users over a decentralized public network, the system comprising: (a) a plurality of member tokens for providing cryptographic capabilities to authenticated users of the decentralized public network; (b) a set of server systems for managing the distribution of the member tokens; (c) means for requesting a member token from at least one server system; (d) a set of client systems, wherein each client system includes (i) means for receiving the requested member token, and (ii) means for utilizing the cryptographic capabilities provided by said member token for selective encryption and decryption; and (e) means for securely distributing a requested member token from at least one server system to at least one client system over the decentralized public network.

53. (Original) The system of claim 52, wherein each client system further includes user authentication means.

54. (Original) The system of claim 52, wherein the means for requesting a member token resides on each client system.

55. (Original) The system of claim 52, wherein means for authenticating a user resides on at least one server system.

56. (Original) The system of claim 52, wherein managing the distribution of the member tokens includes dynamic updating of the member tokens.

57. (Previously Amended) The method or system of claim 1, 4, 7 or 52, wherein the decentralized public network is the Internet.

58. (Previously Amended) The method or system of claim 1, 4, 7 or 52, wherein the decentralized public network is a cellular phone network.